

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION AT CINCINNATI

FILED
JAMES BONINI
CLERK

2003 DEC -2 PM 3: 37

U.S. DIST. COURT
SOUTHERN DIST OHIO
WEST DIV CINCINNATI

UNITED STATES OF AMERICA,

Plaintiff,

v.

DANIEL JEREMY BAAS,

Defendant.

Criminal No.

1:03-cr-00141

STATEMENT OF FACTS

BLOTT

Defendant Daniel Jeremy Baas was employed by Market Intelligence Group (MIG) in downtown Cincinnati from October 2000 until June 2003. He worked as the computer systems administrator.

Acxiom is a customer and information management solutions provider located in Little Rock, Arkansas. Among its clients are 14 of the top 15 credit card issuers, 5 of the top 6 retail banks, 7 of the top 10 automotive manufacturers, 4 of the top 5 telecom companies, and 3 of the top 5 retailers. Its fiscal year 2003 revenue was \$958 million.

Acxiom provided data for MIG to analyze. As part of his duties at MIG, Baas would download files from the directory set aside for MIG on an Acxiom computer. He accessed the Acxiom File Transfer Protocol (FTP) server, located in Conway, Arkansas, with a password.

Baas discovered a file which contained encrypted passwords on the Acxiom FTP server. On the date Baas downloaded the password file, there was no legitimate business activity between Acxiom and MIG that would have necessitated MIG picking up data from FTP.Acxiom.com. He “discovered” the encrypted passwords by accessing the parent directory and searching out the Network Operations (NETOPS) directory from among approximately 3,000 directories. He knew the phrase “NETOPS” would indicate the presence of Acxiom internal processes.

He downloaded the encrypted password file and ran a password cracking program against the file. Baas obtained approximately 300 passwords, and used the “PACKERS” password from the NETOPS directory because it opened all the directories, like a master key. He also could have used specific passwords for specific files, and downloaded data in that way. Armed with the “PACKERS” password, Baas downloaded files that belonged to other Acxiom customers. He exceeded his authorized access by both downloading the password file and then

using the "PACKERS" password to download files containing data belonging to other Acxiom customers.

Baas downloaded Acxiom data from both the MIG office in downtown Cincinnati and from his residence in Milford, Ohio. He stored the downloaded files on compact disks (CDs) which he kept at his residence in Milford. The value of the data exceeded \$5,000. Had Baas been a customer of Acxiom, he would have been charged in excess of \$1.9 million for the data he stole.

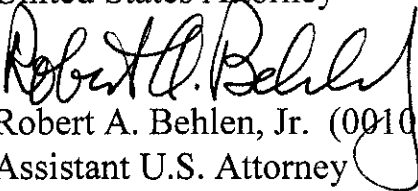
As noted above, Acxiom's customers included national banks and credit card companies. The downloaded files, which belonged to Acxiom's customers, included personal identification information. The data stolen by Baas was not used for criminal or commercial purposes.

The security breach caused by defendant Baas will have cost Acxiom approximately \$4 million by the end of the calendar year. The cost includes employee time (\$2.4 million), travel expenses (\$200,000), and payments for security audits and encryption software (\$1.3 million).

The total cost to Acxiom of Baas's intrusion and theft of data is in excess of \$5.8 million. Both Cincinnati and Milford are located in the Southern District of Ohio.

Respectfully submitted,

Gregory G. Lockhart
United States Attorney


Robert A. Behlen, Jr. (0010695)
Assistant U.S. Attorney
400 Atrium Two
221 East Fourth Street
Cincinnati, Ohio 45202-4166
(513) 684-3711
FAX (513) 684-6385
Robert.Behlen@usdoj.gov
Counsel for the United States